Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

16 nov, 2026 · @Gabriel

Objectif : *disposer à tout moment d'une liste vérifiée de résolveurs DNS éthiques et opérationnels, savoir tester en une minute si un résolveur répond, et réagir quand l'un d'eux ferme ou change ses conditions.*

- ***Public visé :*** *tous publics*
- ***Temps estimé :*** *10 minutes*
- ***Difficulté :*** ★☆☆☆☆ *(Très facile)*
- ***Prérequis :*** *savoir ouvrir un terminal (Linux Mint, macOS) ou l'invite de commandes (Windows)*
- ***Fiches associées :*** *N°6 (changer de DNS), N°20a (WireGuard), N°20c (AdGuard Home), N°30 (box et routeur), N°38 (Pi-hole)*

PARTIE 1 : LES BASES (pour débutants)

1. Le problème : les résolveurs DNS ferment ou changent

Le résolveur DNS est l'annuaire qui transforme un nom (`exemple.fr`) en adresse. S'il ne répond plus, aucun site ne s'ouvre, même si votre connexion fonctionne. Or, depuis 2025, plusieurs résolveurs recommandés partout ont fermé ou changé leurs conditions :

Date	Ce qui s'est passé	Conséquence
24 novembre 2026	Quad9 cesse de répondre en France, après une décision de justice	Toutes ses adresses sont concernées, avec ou sans filtrage, en IPv4 comme en IPv6 (liste en section 2)
2 novembre 2026	Mullvad ferme son service DNS public	194.242.2.2 ne répond plus
15 mars 2025	FDN réserve son DNS classique à ses adhérents, après une attaque	80.67.169.12 et 80.67.169.40 ne répondent plus pour le public ; le DNS chiffré de FDN reste ouvert
Depuis 2024	Cloudflare et Google bloquent certains sites sur décision de la justice française	Ces résolveurs ne sont plus neutres en France

Le risque : un matin, plus aucun site ne s'ouvre chez vous ou chez les personnes que vous aidez, et personne ne comprend pourquoi.

Le bénéfice : une liste vérifiée, un test d'une minute, et un résolveur de secours toujours prêt. Les autres fiches DNS du guide renvoient vers celle-ci, mise à jour à chaque changement.

2. La liste tenue à jour (vérifiée le 16 novembre 2026)

Notre choix par défaut, quand l'appareil ne demande que des adresses IP (box, réglages réseau, Pi-hole, WireGuard) :

- **DNS principal : 45.67.81.23** (Aquilenet)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

- **DNS secondaire : 89.234.141.66** (ARN)

Deux associations différentes, membres de la fédération FFDN (fournisseurs d'accès associatifs) : si l'une tombe en panne, l'autre prend le relais.

Résolveurs associatifs français, sans filtrage

Résolveur	Qui	Adresse IP	DNS chiffré	État
Aquilenet « dns »	Association bordelaise (FFDN)	45.67.81.23	DoT : `dns.aquilenet.fr` ; DoH : `https://dns.aquilenet.fr/dns-query`	✅ Testé le 16/11/2026, aussi depuis un serveur ; vérifie DNSSEC ; sans journaux, 200 requêtes par seconde
Aquilenet « gaia »	Association bordelaise (FFDN)	185.233.100.100	Non	✅ Testé le 16/11/2026 ; environ 20 requêtes par seconde
Aquilenet « hades »	Association bordelaise (FFDN)	185.233.100.101	Non	✅ Testé le 16/11/2026 ; environ 20 requêtes par seconde
ARN	Association strasbourgeoise (FFDN)	89.234.141.66	Non (DoH annoncé)	✅ Testé le 16/11/2026 ; vérifie DNSSEC ; n'enregistre pas les sites visités
FDN	Association (FFDN), depuis 1992	Réservées aux adhérents	DoT : `ns0.fdn.fr` ; DoH : `https://ns0.fdn.fr/dns-query`	✅ En DNS chiffré uniquement

gabriel.ananda@mailo.com

Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

Autres résolveurs européens, sans filtrage

Résolveur	Qui	Adresses IP	DNS chiffré	Remarque
dns.sb	Hébergeur allemand	185.222.222.222, 45.11.45.11	DoT : `dot.sb`	30 serveurs
DNSForge « Blank »	Particulier allemand	138.199.149.249, 78.47.71.194	DoT : `blank.dnsforge.de`	
LibreDNS	Collectif	88.198.92.222, 192.71.166.92	DoT : `dot.libredns.gr`	
DNS4All	SIDN, registre néerlandais du .nl	194.0.5.3, 194.0.5.64	DoT : `dot.dns4all.eu`	⚠️ Service en test, peut être retiré sans préavis

Résolveurs qui filtrent (publicités, sites dangereux, contenus pour adultes)

Résolveur	Adresses IP	Ce qui est bloqué	Remarque
DNS4EU « Protective »	86.54.11.1, 86.54.11.201	Sites malveillants	⚠️ Financé par une subvention européenne ; son opérateur, Whalebone, était visé avec Quad9 et Google par l'ordonnance du tribunal judiciaire de Paris du 13 mai 2026 : il appliquera sans doute les blocages judiciaires français (fiche N°6)
DNS4EU « Child Protection & Ad Blocking »	86.54.11.11	Malveillants, adultes, publicités	Même réserve
DNSForge (normal)	49.12.67.122, 91.99.154.175	Publicités, traqueurs, malveillants	Particulier allemand ; limité à 100 requêtes par 10 secondes
DNSForge « Clean »	49.12.223.2, 49.12.43.208	Le même, plus adultes et paris	
HaGeZi « root »	188.34.161.210 (DoT : `root.hagezi.org`)	Publicités, traqueurs, télémétrie, arnaques, malveillants	Particulier allemand, auteur de listes de blocage réputées ; sans journal des requêtes ; ✅ testé le 16/11/2026

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

Résolveur	Adresses IP	Ce qui est bloqué	Remarque
HaGeZi « juuri »	95.217.163.17 (DoT : `juuri.hagezi.org`)	Le même, serveur en Finlande	À mettre en DNS secondaire avec « root »
HaGeZi « ctif »	162.55.58.40 (DoT : `ctif.hagezi.org`)	Menaces seulement (arnaques, malveillants)	Sans blocage des publicités

À tester avant usage (listes communautaires anciennes)

Ces résolveurs figurent dans les listes de la FFDN et de DIY ISP, mises à jour pour la dernière fois en décembre 2023. Testez-les (section 3) avant de les conseiller.

Résolveur	Adresse IP	Pays
LDN (association lorraine, FFDN)	80.67.188.188	France
log.bzh (hébergé chez Grifon, FFDN)	80.67.190.200	France
censurfridns	91.239.100.100	Danemark
dns.as250.net	194.150.168.168	Allemagne

Ne plus utiliser

Résolveur	Adresses	Pourquoi
Quad9	9.9.9.9, 149.112.112.112, 9.9.9.10, 149.112.112.10, 9.9.9.11, 149.112.112.11, 2620:fe::fe, 2620:fe::9, 2620:fe::10, `dns.quad9.net`	Ne répond plus en France depuis le 24 novembre 2026, sans filtrage compris. Quad9 n'a pas précisé comment les requêtes venant de France seront refusées
Mullvad	194.242.2.2 et suivantes	Fermé le 2 novembre 2026
FDN en DNS classique	80.67.169.12, 80.67.169.40	Réservé aux adhérents depuis mars 2025 (le DNS chiffré reste ouvert)
Cloudflare, Google	1.1.1.1, 8.8.8.8	Américains ; bloquent des sites sur décision de la justice française (Google était visé par la même ordonnance que Quad9)
OpenDNS	208.67.222.222	Inaccessible depuis la France

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

Avant de commencer

- ☐ Vous avez noté l'adresse du résolveur à tester
- ☐ Vous savez ouvrir un terminal : **Menu › Terminal** sous Linux Mint, **Applications › Utilitaires › Terminal** sous macOS, touche **Windows** puis tapez **cmd** sous Windows
- ☐ Vous êtes connecté à Internet

3. Tester un résolveur en une minute

1. Ouvrez le terminal (ou l'invite de commandes sous Windows), puis tapez `nslookup example.org 45.67.81.23` en remplaçant l'adresse par celle du résolveur à tester.
    - Vous devez voir : une ligne **Non-authoritative answer:** suivie d'adresses. Le résolveur fonctionne.
2. Si vous voyez **timed out**, **host unreachable** ou **no servers could be reached**, recommencez une fois.
    - Vous devez voir : le même message. Le résolveur ne répond pas depuis votre connexion : choisissez-en un autre dans la liste.
3. Pour vérifier qu'il contrôle les signatures DNSSEC (protection contre les fausses réponses), tapez `nslookup dnssec-failed.org 45.67.81.23`.
    - Vous devez voir : **SERVFAIL** ou **server can't find**. C'est la bonne réponse : ce domaine a une signature volontairement fausse, et un résolveur qui vérifie DNSSEC le refuse. Si vous obtenez une adresse, le résolveur ne vérifie pas DNSSEC.
4. Pour un résolveur qui bloque les publicités, tapez `nslookup pagead2.googlesyndication.com 188.34.161.210` en remplaçant l'adresse par celle du résolveur.
    - Vous devez voir : **0.0.0.0**. Le domaine publicitaire est bloqué. Si vous obtenez de vraies adresses, le résolveur ne filtre pas les publicités.
5. Sur votre serveur (WireGuard, Pi-hole), faites le même test : un résolveur peut répondre chez vous et pas depuis un hébergeur.
    - Vous devez voir : les mêmes résultats.

Tester un DNS chiffré :

- **Android** : **Paramètres › Réseau et Internet › DNS privé**, saisissez `dns.aquilenet.fr` ou `ns0.fdn.fr`. Si Android affiche **Impossible de se connecter**, le résolveur ne répond pas.
- **Firefox** : réglez le DNS via HTTPS (fiche N°6), puis ouvrez un site. S'il ne s'ouvre pas, revenez au réglage par défaut et choisissez un autre résolveur.
- Dans tous les cas, un test de fuite DNS (fiche N°6) vous dit quel résolveur vous utilisez réellement.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

4. Comment choisir

Critère	Ce que nous recommandons
Qui le gère	Une association ou un collectif plutôt qu'une entreprise qui vit de vos données
Où	En France ou en Europe, hors du droit américain (Cloud Act)
Filtrage	Aucun, sauf si vous voulez bloquer publicités ou contenus pour adultes (choix assumé)
Journaux	Pas d'enregistrement des sites visités, annoncé publiquement
DNSSEC	Vérifié (test section 3)
Secours	Toujours deux résolveurs de fournisseurs différents

5. Dépannage

Symptôme	Cause possible	Action
Plus aucun site ne s'ouvre, mais la connexion semble active	Le résolveur ne répond plus	Testez-le (section 3) ; remplacez-le par un résolveur de la liste
Depuis le 24 novembre, plus aucun site sur le téléphone ou sur tous les appareils de la maison	Quad9 est encore réglé dans la box, le routeur, le « DNS privé » du téléphone ou le DNS chiffré du navigateur (`dns.quad9.net`)	Remplacez-le partout : box (fiche N°30), ordinateur et téléphone (fiche N°6), navigateur (Firefox : **Paramètres › Vie privée et sécurité › DNS via HTTPS** ; Chrome : **Paramètres › Confidentialité et sécurité › Sécurité › Utiliser un DNS sécurisé**) ; n'oubliez pas les adresses IPv6
Certains sites seulement ne s'ouvrent pas	Le résolveur bloque ces sites (filtrage ou décision de justice)	Testez avec un résolveur sans filtrage
Le test répond chez vous mais pas sur le serveur	Le résolveur est réservé à certains réseaux, ou bloque les hébergeurs	Choisissez-en un autre pour le serveur
Lenteurs aux heures chargées	Limite de requêtes atteinte (environ 20 par seconde sur certains serveurs d'Aquilenet)	Préférez 45.67.81.23 (200 par seconde) ou installez un résolveur local (fiche N°20c ou N°38)
Android : **Impossible de se connecter** au DNS privé	Le DNS chiffré ne répond pas	Essayez un autre nom (`ns0.fdn.fr`, `dns.aquilenet.fr`) ou repassez en **Automatique**

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

PARTIE 2 : ALLER PLUS LOIN (pour intermédiaires et avancés)

6. Où se tenir informé

Ces listes sont tenues par d'autres que nous. Avant de suivre l'une d'elles, testez toujours le résolveur (section 3) : une liste peut avoir un train de retard, comme pour FDN.

Source	Ce qu'elle apporte	Mise à jour
Wiki de sebsauvage	Liste commentée en français, résolveurs déconseillés barrés	Régulière (dernière : 23 octobre 2026)
Wiki de la FFDN	Résolveurs ouverts des associations de la fédération	Ancienne (décembre 2023)
Wiki de DIY ISP	Résolveurs associatifs européens, avec la vérification DNSSEC	Ancienne (décembre 2023)
Wiki du projet curl	Plusieurs centaines de résolveurs chiffrés (DoH), testés un par un	Régulière, en anglais
Pages officielles d'Aquilenet, d'ARN et de FDN	Adresses et conditions à la source	À consulter en cas de doute

7. Ne plus dépendre de personne : votre propre résolveur

Un résolveur installé chez vous ou sur votre serveur interroge directement les serveurs racines d'Internet, sans intermédiaire. Plus aucune fermeture extérieure ne vous concerne.

- **Unbound** : le résolveur libre de référence, à installer sur un Raspberry Pi avec Pi-hole (fiche N°38) ou sur votre serveur.
- **AdGuard Home** (fiche N°20c) : peut interroger plusieurs résolveurs à la fois et passer automatiquement au suivant si l'un ne répond plus.

Pour tester plus finement depuis Linux, la commande `dig` (paquet `bind9-dnsutils`) affiche le drapeau **ad** quand la réponse est vérifiée par DNSSEC :

```
dig +dnssec example.org @45.67.81.23
```


gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

8. Journal des mises à jour de cette fiche

Date	Changement
16 novembre 2026 (V1.0)	Création de la fiche. Choix par défaut : Aquilenet (45.67.81.23) et ARN (89.234.141.66). FDN en DNS chiffré uniquement. Quad9, Mullvad, Cloudflare et Google déconseillés
16 novembre 2026 (V1.1)	Test DNSSEC réussi sur Aquilenet (45.67.81.23) et ARN (89.234.141.66) ; Aquilenet répond aussi depuis un serveur hébergé
16 novembre 2026 (V1.2)	Ajout des résolveurs filtrants de HaGeZi (testés : bloquent bien les domaines publicitaires) ; test du blocage des publicités en section 3
16 novembre 2026 (V1.3)	Quad9 : liste complète des adresses coupées (variantes sans filtrage et IPv6 comprises) ; rappel de vérifier la box et le téléphone
16 novembre 2026 (V1.4)	Journal des mises à jour remis dans l'ordre chronologique
16 novembre 2026 (V1.5)	Quad9 : vérifier aussi le DNS chiffré du navigateur. DNS4EU : son opérateur Whalebone était visé par l'ordonnance du 13 mai 2026 et appliquera sans doute les blocages judiciaires français

À savoir avant de se lancer

Crainte fréquente	La réalité
« Changer de DNS, c'est risqué »	Le test d'une minute vous dit si ça marche ; revenir en arrière prend 30 secondes
« Une petite association, ce n'est pas fiable »	C'est pour cela qu'on en met deux, de fournisseurs différents
« Les gros (Google, Cloudflare) sont plus sûrs »	Ils sont rapides, mais américains et bloquent déjà des sites en France
« Je dois tout refaire à chaque fermeture »	Non : cette fiche est mise à jour, il suffit de changer une ou deux adresses

Challenge 7 jours

1. Jour 1 : testez le résolveur que vous utilisez aujourd'hui (section 3).
2. Jour 2 : testez Aquilenet (45.67.81.23) et ARN (89.234.141.66).
3. Jour 3 : faites le test DNSSEC sur les deux.
4. Jour 4 : réglez-les sur votre ordinateur ou votre box (fiches N°6 et N°30).
5. Jour 5 : réglez le DNS chiffré sur votre téléphone (`dns.aquilenet.fr` ou `ns0.fdn.fr`).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

6. Jour 6 : faites un test de fuite DNS pour vérifier le résultat.
7. Jour 7 : notez dans votre agenda de revenir sur cette fiche dans trois mois.

Vous allez constater : qu'un résolveur se teste en une minute, et que vous n'êtes plus à la merci d'une fermeture surprise.

En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Utiliser Aquilenet et ARN	Deux résolveurs associatifs, sans filtrage, ouverts à tous	Section 2
Tester avec `nslookup`	Savoir en une minute si un résolveur répond	Section 3
Tester DNSSEC	Être protégé des fausses réponses	Section 3
Garder un secours	Ne jamais rester sans Internet	Section 4
Consulter cette fiche régulièrement	Être prévenu des fermetures	Section 8

À retenir absolument

- Un résolveur DNS peut fermer ou changer ses conditions du jour au lendemain : gardez-en toujours deux, de fournisseurs différents.
- Notre choix par défaut : 45.67.81.23 (Aquilenet) et 89.234.141.66 (ARN) ; en DNS chiffré, `ns0.fdn.fr` ou `dns.aquilenet.fr`.
- `nslookup example.org` ADRESSE dit en une minute si un résolveur répond.
- N'utilisez plus Quad9 (aucune de ses adresses), Mullvad, ni les adresses IP de FDN, et vérifiez partout : box, ordinateur, téléphone et DNS chiffré du navigateur.

Test final :

1. Vous savez tester un résolveur avec `nslookup` ✅
2. Vos appareils utilisent deux résolveurs de fournisseurs différents ✅
3. Le test DNSSEC renvoie **SERVFAIL** sur `dnssec-failed.org` ✅
4. Vous savez où trouver la liste à jour ✅

Références

- Aquilenet – Résolveurs DNS ouverts à tous (adresses, limites)
- Aquilenet – dns.aquilenet.fr (DoH, DoT, absence de journaux, 200 requêtes par seconde)
- ARN (Alsace Réseau Neutre) – Résolveur DNS libre et ouvert
- FDN – Résolveurs DNS ouverts (adresses, DoT, DoH)
- FDN – Renforcement des protections des serveurs DNS (mars 2025)
- Quad9 – Au revoir, France (fin du service en France le 24 novembre 2026)

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°93 : Trouvez un résolveur DNS qui fonctionne – la liste tenue à jour V1.5

- IT-Connect – Quad9 quitte la France (ordonnance visant aussi Google et Whalebone, opérateur de DNS4EU)
- DNS4EU – Adresses, DoH et DoT pour le public
- DNS4All (SIDN Labs) – Adresses et conditions
- Wiki de sebsauvage – Résolveurs DNS alternatifs (mis à jour le 23 octobre 2026)
- Wiki de la FFDN – Résolveurs DNS ouverts des membres
- Wiki de DIY ISP – Résolveurs DNS ouverts
- GitHub – HaGeZi, résolveurs DNS filtrants (adresses, journaux, licence)
- GitHub – HaGeZi, aide-mémoire des adresses (IPv4, DoT, DoH)
- curl – Liste des serveurs DNS-over-HTTPS publics

gabriel.ananda@mailo.com
CC BY SA